



Three-strikes
rule hits a
few snags 10

Critics heap
scorn on child-
protection plan 11

Headset that
lets PCs read
your mind 12



Security flaws found in BT's Home Hub

Surfers using the UK's most popular WiFi router are at risk of having their networks hacked because the default security settings installed are too easy to guess. According to white hat hackers at GNUCitezen.org, many home routers manufactured by Thomson/Alcatel – including BT's Home Hub – use weak algorithms to generate the security keys that lock down WiFi networks.

"Many of us involved in researching the security of wireless home routers have always suspected that routers that come with default Wired Equivalent Privacy (WEP) and WiFi Protected Access (WPA) keys

follow predictable algorithms for practical reasons," said the report author Adrian Pastor. "I'm talking about routers that come with those stickers that include information such as the serial number, the default SSID and the default WEP and WPA key."

"If you own a wireless router that uses a default WEP or WPA key, such keys can be predicted based on publicly available information such as the router's MAC address or SSID," Pastor said. "It's quite likely that the bad guys can break into your network if you're using the default encryption key. Our suspicion that such issues exist on the BT Home Hub has been confirmed."

Using simple techniques, WEP keys can be narrowed down to just 80 possibilities. Consumers who use the more robust WPA to secure their BT Home Hub are also at risk, because the algorithm uses a predictable means to determine the WPA key.

BT says it is aware of the problem, but played down the threat to consumers. "We are aware of this problem, although we don't believe that any customers have been affected," said a BT spokesperson. "It's important to realise that although it has been possible to demonstrate a theoretical scenario where the hub may be vulnerable, we don't believe it is something that should affect the majority of BT customers in real life."

However, now that the vulnerability has been discovered, hackers have wasted no time in testing out the theory. "I just tried this at home (several of my neighbours appear to have Home Hubs), and it works perfectly," wrote one GNUCitezen contributor.

BT suggests that anyone who has a Home Hub should change the encryption type from WEP to WPA (and change the default encryption key), and should also follow the other instructions that are listed at www.bt.com/help/hub. The same advice is worth following for all home routers.



▲ Security fears rise over home router encryption keys

First handheld Atom lands in Japan

Sharp has unveiled the first mobile phone and handheld computer based on Intel's Atom platform. The bulky D4 has a powerful specification for a phone, with a 1.33GHz Atom Z520 processor and 1GB of 533MHz DDR2 memory. It runs Windows Vista Home Premium Service Pack 1 and will be available on Japan's Willcom network for around £600.

At 470g the device is hefty, but it has a 40GB hard disk, WiFi, a slide-out Qwerty keyboard and a tilting screen that the manufacturer says makes it easier to read when typing on a flat surface. According to Intel, 40 similar devices are on the drawing board, so even if the D4 fails to make it to Europe after its June launch, similar devices are likely to be available by the end of the year.



▲ Sharp's D4 handheld computer is leading the charge for the Intel Atom platform

CONTACTS

To contact the *Computer Shopper* newsdesk, please send an email to news@computershopper.co.uk.

You can also write to us at:

News
Computer Shopper
30 Cleveland Street
London
W1T 4JD

For daily news, please visit
www.computershopper.co.uk

Web TV moves into mainstream

New hardware devices for streaming video straight into the living room could do for television what MP3 players did for music, according to experts that predict an impending surge in programming over the internet.

One such device is a set-top box from Myka that acts just like a Sky, cable or Freeview box, but plugs in to the internet to receive its content via BitTorrent. The box, which includes a hard disk, is expected to make P2P video downloading extremely simple. The concept could put a huge strain on bandwidth resources if it proves as popular as the BBC's iPlayer catch-up TV service.

Although the company is in talks with content providers, Myka owners will be able to download, legally or illegally, any content found on the web in MPEG2, H.264, WMV and DivX formats. "The rise of services like this will start to challenge television itself," said Suranga Chandratillake, CEO of video search company Blinkx. "How they respond to the challenge will be interesting. Can they give people what they want, free or at the right price, or will it go the [same] way [as] the music industry?"

Internet television and video has been touted for years, but until recently it has remained niche because it required more effort than watching TV and often involved grainy, clunky footage.

"This is not unlike iPlayer, which is mass-market, but could be even bigger because it



▲ Everyone can be a time lord now IPTV has ripped up the schedule for programmes such as *Doctor Who*

doesn't need a computer," said Jake Ward, a director of media company Broadview. "The Myka and Apple TV could make this mainstream, and could really change the way we watch television, with lots more content. If it goes mainstream, we are in for big changes."

The news will make uncomfortable reading for ISPs, who are already complaining about the

extra traffic generated by the iPlayer. PlusNet said it has seen some of its costs rise threefold since iPlayer launched, while Telco 2.0 said the service "blows up" the ISP business model. Many ISPs hire expensive IPStream pipes to carry data, with a capacity of just 155Mbit/s. Watching iPlayer eats 500Kbit/s, so if 300 people watch simultaneously, an ISP's IPStream pipe is filled.

Mixed messages on cyberwar

Security officials have supplied contrasting views on the cyberterrorism threat. At its annual meeting in Bucharest, NATO announced a Cyber Defense Management Authority (CDMA) to safeguard the organisation's critical networks.

According to NATO officials, the new CDMA is charged with managing "immediate and effective cyber defence action where appropriate".

The cyberwarriors are responsible for planning NATO's Computer Incident Response, established after last year's allegedly Russian-led cyberattacks on Estonian government and strategic targets. Opinion is split on the identity of the perpetrators, but the impetus has pushed the issue of cyberterrorism on to NATO's main agenda.

This will come as a shock to UK officials. Stephen Cummings, director of the UK's Centre for the Protection of National Infrastructure, told a Royal United Services Institute meeting there was no evidence that terrorists planned cyberattacks.

"Discussion of cyberterrorism distracts our attention from the more pressing terrorist threats, which are still physical," he said in a presentation that, according to Reuters, included a slide that said 'Cyberterrorism is a myth'.

Shopper survey uncovers the true speed of broadband

The true speed of UK broadband is 3.6Mbit/s, according to the extensive survey we launched in *Shopper* 243. With more than 22,000 people taking part as we went to press, this is the UK's biggest survey to take into account broadband speed and customer satisfaction. The results will appear in next month's issue, with each ISP's performance exposed. However, we wanted to give a sneak preview of some of the headline statistics.

On average, our readers pay for a broadband speed of 6.6Mbit/s, which suggests that most people get just over half their advertised speed.

Most readers seem happy with the deal they are getting at the moment, with 77 per cent not planning to change suppliers – although our results could well change that – and 70 per cent willing to recommend their supplier to a friend. Reliability seems high for most readers, with only 2.5 per cent of people rating their connection poorly.

Things get more interesting when considering technical support. Just over 50 per cent of people who have had to phone for support rated it average or below, with 12 per cent rating the service as very poor.

As we went to press, the survey had a few more days to run. Once it has closed, we'll analyse the results, which we'll publish next month. For each ISP, we'll let you know how fast each connection speed it offers really is, how many people rate its technical support and how other users rate the overall service. Make sure you don't miss the results.



▲ *Computer Shopper's* broadband survey is the biggest of its kind and has thrown up some very interesting results

IN BRIEF

MAC ATTACK

A US company is risking the wrath of Apple by selling a \$399 (£200) Mac clone running a hacked version of OS X Leopard. Apple guards its rights jealously, citing the stability benefits of one-company software-hardware integration and bans the use of Leopard on "any non-Apple-labelled computer".

Rogue vendor Psystar vowed to continue selling its Open Computer because it believes Apple's policy violates US competition laws. "What if Microsoft said you could only install Windows on Dell computers?" a Psystar spokesperson asked.

PIRATE PLEA

Download search site Pirate Bay has demanded a cheeky cash settlement from the International Federation of the Phonographic Industry (IFPI) after the music business body persuaded a Danish court to order ISPs to block access to the site. Pirate Bay is seeking compensation for lost revenue, and says it will use any payment received to fund aspiring artists.

DIRTY WORK

This month's award for pointlessly obvious research goes to security firm ScanSafe, which has shockingly revealed that laptop users working away from the office are two and half times more likely to use pornography sites than office-bound colleagues, and several times more likely to visit extreme websites.

BATTERY BONANZA

Laptop users are set for a battery boost after the announcement of technology from the Argonne National Laboratory that developers say could increase running time by 30 per cent and lead to safer batteries. Japanese company Toda Kogyo is set to start annual production of 30 million units.

ONE MILLION VIRUSES

The internet's virus population has passed the million mark, according to Symantec. The company's Internet Security Threat report revealed that 711,912 new threats were recorded in 2007, up from just 125,243 in 2006, pushing the total number of malicious programs detected to 1,122,311.

Three strikes rule hits snags

Plans by music industry officials and politicians to instigate a 'three strikes and you're out' rule to block illegal downloaders have run into trouble on two fronts, with lawmakers and ISPs both slamming the proposals.

The plan to cut off users' internet connections after three warnings came at the behest of the music industry and has won support in the corridors of power, but was vilified by consumers.

Now MEPs have said the plans to cut file-sharers from the web go against "civil liberties and human rights" and voted against the proposal.

"The vote shows that MEPs want to strike a balance between the interests of rights holders and those of consumers, and that big measures such as cutting off internet access shouldn't be used," said a European Parliament spokeswoman in a statement.

Although seen as a victory for consumer rights, the vote carries little legal weight in Britain. The government could still impose the measures in the UK, and maintains it will do so "if ISPs and the music industry can't come up with some sort of self-regulation".

ISPs are reluctant to take on the expense of policing the internet. The boss of Talk Talk's parent company, Carphone Warehouse, launched a scathing attack on the plans. "We are the conduit that gives users access to the internet, we do not control the internet nor do we control what our users do on the internet. I cannot



▲ Trouble in ISP-land as music industry and government anti-piracy plans face criticism

foresee any circumstances in which we would voluntarily disconnect a customer's account on the basis of a third party alleging a wrongdoing," said chief executive Charles Dunstone.

"We believe that a fundamental part of our role as an internet service provider is to protect the rights of our users to use the internet as they choose. The music industry has consistently failed to adapt to changes in technology and now seeks to foist its problems on someone else."

Dunstone said Talk Talk would take legal steps to defend its customers.

Windows could collapse, say analysts

Microsoft's Windows operating system is in danger of collapsing under its own weight unless the company makes radical changes, according to respected research firm Gartner.

In a presentation entitled "Windows Is Collapsing: How What Comes Next Will Improve", analysts Michael Silver and Neil MacDonald said Microsoft had not responded to changes in the market and was so hampered by the need to include its own legacy software that it was not fit for purpose.

"Apple introduced its iPhone running OS X, but Microsoft requires a different product on handhelds because Windows Vista is too large, which makes application development, support and the user experience all more difficult," they said. "Windows as we know it must be replaced."

"For Microsoft, its ecosystem and its customers, the situation is untenable," they added, highlighting the fact that Windows Vista was poorly received despite a five-year wait for the software.

What users want, the analysts argued, is a lightweight software package largely delivered over the web. Companies such as Google seem to be muscling in on the software giant's space with free web-based tools such as the Google Docs office suite.

The critics also said a move towards cheaper, less capable computers left Windows, which requires hefty hardware, exposed. Microsoft defended its software, and said Gartner's research for the report was not up to scratch.

Mesh mess leaves customers confused

UK PC manufacturer Mesh is embroiled in a warranty service dispute that customers claim will leave them out of pocket and without cover for their computers.

Mesh used a company called Repair-Line to undertake service, paying it £5 per computer to take on the collection, repair and return of Mesh computers. However, the companies fell out when Mesh withheld payments after a contractual dispute.

According to a post on Repair-Line's website, "all services to the manufacturer are being withheld due to non-payment of account and failure to exchange parts buffer stock to allow repairs to continue".

Customers who paid for onsite warranties for up to three years say Mesh has told them the money is now

wasted, and that they have been advised to sign up with Mesh's new contractor, OrderWork.

Confusion reigns, however, as Mesh told *Computer Shopper* that it would honour all warranties issued by the company.

"I don't know what the fuss is about," said a Mesh spokesperson. "We've fallen out with our contractor and have appointed another one. We'll be honouring all warranties people have bought for Mesh machines."

Yet that response is a far cry from experiences reported by readers, who have told *Computer Shopper* that both Mesh and Repair-Line were refusing to undertake work on faulty machines at the time of going to press. The case continues.



Critics pour scorn on child-protection plan

Government plans to protect children by banning sex offenders from social-networking sites have come under fire for being naïve and unworkable.

Under new plans to monitor sex offenders online, the Home Office says the email addresses of registered child sex offenders will be passed by police to social-networking websites, enabling the sites to stop the offenders visiting.

Home Secretary Jacqui Smith said the government was "working together with police, industry and charities to create a hostile environment for sex offenders on the internet and [is] determined to make it as hard for predators to strike online as in the real world".

However, parenting groups ridiculed the proposals, suggesting they would be too easy for criminals to circumvent. "Doesn't this sound like a good idea," said a spokesperson for the Parents Organisation, unable to hide his sarcasm. "Of course, sex offenders won't be clever enough to declare one address and then sign up to any of the available – accessible from anywhere and

any computer – webmail accounts. So who will police this? Truth is, this is another idea that looks great on paper, makes for great headlines and promises much but is incapable of delivering."

The Home Office responded to criticisms by stating that stiff penalties would stop offenders breaking the regulations.

"A sex offender will need to notify the police of any new email address," a spokesperson told *Computer Shopper*. "It will be a criminal offence, punishable with up to five years imprisonment, to use an email address that has not been notified to the police."

But critics point out that if a sex offender is not concerned about the consequences of breaking child sex laws, they are unlikely to be worried about flouting email regulations.

Regardless of the obvious flaws, police officials welcomed the move, saying the legislation would give them greater powers when they did discover paedophiles using social-networking sites.

High definition goes on crash diet

High-definition (HD) video could soon be available over the internet to millions of homes, thanks to a breakthrough technology that reduces the bandwidth needed to transfer it, according to developers.

Broadcast International and IBM have demonstrated that HD video can be slimmed to fit down most UK ADSL connections.

"The ability to squeeze more video on to less bandwidth is the number one priority in the industry," said Rod Tiede, CEO of Broadcast International.

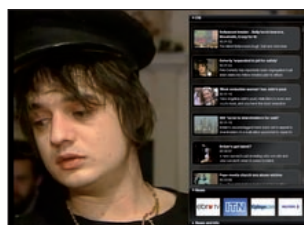
Most HD video is currently transmitted at nearly 20Mbit/s,

which is far too fast for most domestic broadband connections, but clever management of codecs and improved server technology has crammed content into less than 3Mbit/s, the companies claim.

Broadcast International's CodecSys compression software analyses a video stream and decides which codec is best-suited for a particular video sequence.

According to Tiede, specialist codecs are designed to handle particular types of high-bandwidth video frames or streams, such as fast sequences in sport or explosions in action movies.

"Those shots are extremely bandwidth-intensive and pose chokepoints to generalist codecs," he said. "Using specialist codecs for the job, CodecSys is able to eliminate these chokepoints."



▲ New codecs promise HD video over broadband connections

Ofcom and BT hint at fibre network

Internet users who are struggling with slow broadband speeds could see dramatic improvements in future after two big-hitting players hinted at the possibility of rolling out a national fibre network.

Telecoms regulator Ofcom said the government had to take some responsibility for forcing the issue of a £20 billion network overhaul.

Ofcom CEO Ed Richards, speaking to the Institution of Engineering and Technology, said that it was a matter of how and when, and not whether, it would happen. "Market players, the regulator and government all have a part to play. There is no single application or magic regulatory solution that will guarantee mass deployment and mass migration overnight," he warned.

BT, the major stakeholder in Britain's telecommunication network, also appeared to be softening its stance when its new chief



▲ Ofcom CEO Ed Richards

executive, Ian Livingston, suggested that his company would be willing to lay fibre, but only if the regulator made changes to the Universal Service Obligation (USO), which forces BT to provide services to the entire country and make them available to rival ISPs.

"We want changes to the USO to reflect a fibre world," Livingston told the *Sunday Times*. "There are 200-odd service providers. Why should all the USO fall on BT Retail?"

And in a thinly veiled threat to the regulator, Livingston insisted the investments were unjustifiable unless the regulations changed to allow it to target high-population density areas. "We will not spend material amounts of money that will guarantee that we lose money for shareholders," he said.

The result could mean that cities and towns benefit from super-fast broadband, while rural areas remain in a bandwidth slow lane.

IN BRIEF

TESCO LAUNCHES ITUNES RIVAL

Tesco plans to go head to head with iTunes when it launches a music, film, TV and games download service this month. The supermarket giant says it will expand its existing service to offer 3.3 million music tracks on both Apple and Windows platforms, but the company didn't reveal details of pricing.

QUICK STEP FOR MUSIC FILE SIZES

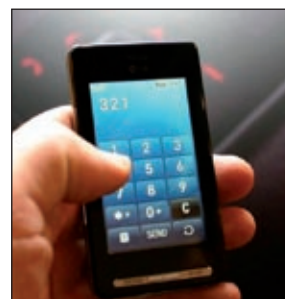
Boffins at the University of Rochester in the US have found a way of recording music to a file that is 1,000 times smaller than an equivalent MP3. The researchers recorded a 20-second clarinet solo in less than a kilobyte by mimicking the physics of both the clarinet and the musician. They claim the system replays music through the computer by re-creating the original performance, rather than replaying a recording.

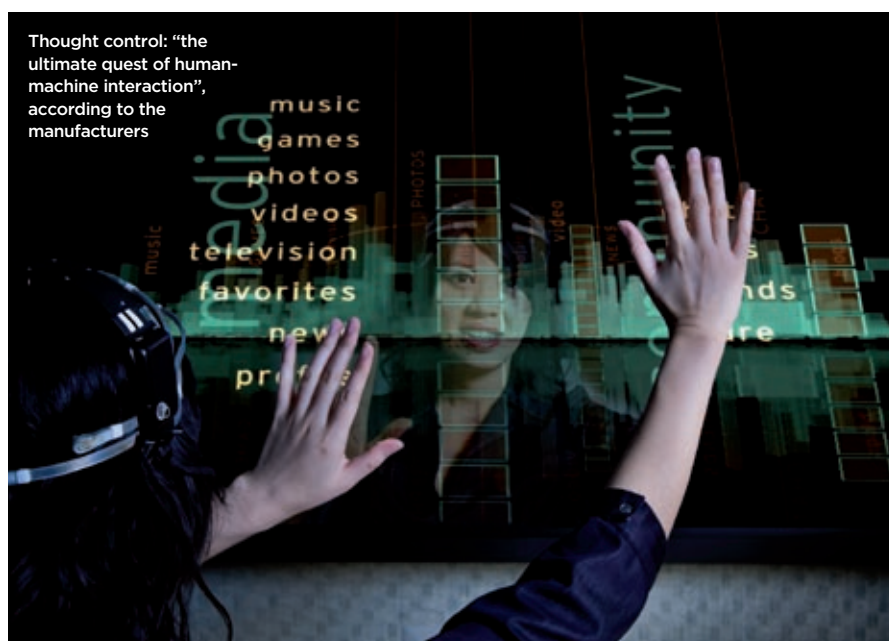
SHIPS WRECKED INTERNET CABLES

Two ships suspected of cutting undersea internet cables have been detained in Dubai after the cable company tracked down satellite images that showed the vessels in the area at the time of the alleged attack. The damage to the cables reduced the capacity of the Middle East's internet capability by 70 per cent before traffic was rerouted.

UNPROTECTED TEXT INJURES MILLIONS

Six million Britons have injured themselves while texting or making calls on mobile phones, according to a survey from phone directory service 118 118. According to the survey, the chief culprits were lamp-posts, bollards and bins, with injuries ranging from minor cuts to broken skulls. The phenomenon has led to the installation of padded lamp-posts in London's Brick Lane.





Thought control: "the ultimate quest of human-machine interaction", according to the manufacturers

PCs to read your mind

After years of frustrating liaison with keyboards, flitty track pads and rowdy mice, consumers could soon tell computers exactly what they want them to do just by thinking.

A trio of companies are on the verge of releasing neural interfaces that will enable users to play games, scroll through menus or choose music through thought control alone.

Emotiv is beta-testing its Epoc headset; OCZ says its neural Neural Impulse Actuator is about to go into production; and Neurosky recently demonstrated its Project Millennia headset.

"Controlling a computer with your mind is the ultimate quest of human-machine interaction," said Nam Do, CEO of Emotiv Systems. "When integrated into games, virtual worlds and other simulated environments, this technology will have a profound impact on the user's experience. Since our prototype last year, we've made dramatic technological breakthroughs in order to create the first wearable, affordable brain-controlled gaming headset."



▲ Emotiv's mind-reading Epoc headset is expected to cost around £150

The systems work by reading activity in the brain, the nervous system and muscles, which is captured by the headset and sent to your PC over a USB link.

"The brain is made up of 100 billion neurons," said Do. "When these neurons interact, an electrical impulse is emitted, which can be observed using non-invasive electroencephalography."

"Brain computer interface technology works by observing an individual's electrical brain activity and processing it so that computers can take inputs from the human brain."

The companies claim the techniques work with movements, thought and emotions.

Both the Epoc and NIA devices are expected to retail for \$300 (around £150), but gamers expecting an immediate edge over rivals may be disappointed.

Like speech recognition, users will be expected to teach the software how to work and, like a Jedi, a gamer may need to train their minds.

Phorm faces new hurdles

The tide appears to be turning against the controversial ad-targeting system from Phorm, after the Information Commissioners Office (ICO) insisted that the company ask surfers' permission before harvesting their details for financial gain and critics continued to campaign against the advertising company.

Phorm is proposing a system (being trialled by BT, Virgin Media and Talk Talk) that monitors surfing habits so it can sell advertising that's relevant to individual users. The system has been widely criticised as an invasion of privacy, abuse of position and, in some quarters, illegal.

Although the ICO agreed with Phorm that the company had not appeared to break any laws regarding personal data, it said European laws demand that users must give their explicit consent before any company could use their details to target them with adverts.

"This strongly supports the view that Phorm products will have to operate on an opt-in basis to use traffic data as part of the process of returning relevant targeted marketing to internet users," information commissioner Simon Davis said in a statement.

The proposals from the ICO represent a major spanner in Phorm's works, because it's unlikely that many people would choose to sign up to such a service.

"Being opt-in faces them with a much more difficult business model," said Nicholas Bohm of the Foundation for Information Policy Research, which has branded the system illegal. To make matters worse, F-Secure has hinted that it might include Phorm in its list of blacklisted companies, blocking the software from consumers' computers.



▲ Phorm's plans to target ads at individual users could fall foul of European law

Timeline 150+ years of input devices

QWERTY keyboards

The QWERTY keyboard made its first appearance on Sholes' early typewriter. The ordering of keys was designed to stop them jamming. Modern keyboards have no mechanical parts to snag, but by the time standard 101-key computer keyboards arrived in the 1980s, we were too entrenched.



The mouse

Invented by Douglas Engelbart, whose mouse consisted of two perpendicular wheels. Early mechanical versions gave way to the ball mouse (1972), optical mice (1980) and, by 2004, lasers that could track movement. Confusion still surrounds the correct plural of the noun.



Touch screens

The first touch screen with a transparent surface was made by Elographics, and this super-intuitive control method sparked a revolution that has been a common thread from ATMs to Tablet PCs, Windows Surface table PCs (pictured) and Apple's iPods.



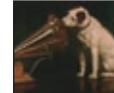
Trackpad

Now the *de facto* leader in laptop mouse replacement, the trackpad was used on the early Apollo desktop computers and controls movement by detecting when a grounded object (such as a finger) disturbs the flow of electricity in the pad.



Software-only dictation

DragonDictate for Windows 1.0 was as coherent as a conversation with Boris Johnson, requiring a pause between each word, but marked a new input option for PCs. By 1997 Dragon and IBM had both launched continuous speech software, although recognition remains erratic.



1860s

1963

1974

1980

1994



Shutterbugs paint a bleak picture

Photographers – from pros and seasoned hobbyists to day-trippers taking snaps of the family on a point-and-shoot camera – are facing an increasingly hostile battle with security officials over the right to take pictures in public.

A 79-year-old man was recently detained by security guards in Hull after taking a digital photograph of his wheelchair-bound wife at the entrance to a new shopping centre. The pair made as unlikely a couple of terrorists as Torvill and Dean, but it was the suspicion that they might be on a bombing campaign that saw their photos deleted.

The security guards were acting on the 66 pages of advice for shopping centres from the National Counter Terrorism Security Office. The case is just one of dozens in which police, community support officers and security officials have asked snappers to delete images from their cameras, moved them on or made arrests and confiscated cameras.

"I was told by staff at the London Eye that I could not take photographs of it for copyright and security reasons," said Simon Taylor, an amateur photographer who has an ongoing e-petition on the Downing Street website promoting photographers' rights.

"Maybe because I was using a tripod they singled me out rather than the hundreds of tourists with handheld cameras, but I'm sure if terrorists wanted a picture of the London Eye, they could find one on the internet, or in any one of thousands of publications."

The perceived persecution has been exacerbated by police chiefs issuing posters warning the public to be wary of people taking photographs in case they were terrorists and by discarded proposals from Ken Livingstone to put 'No photography' signs up in London parks to warn parents about people taking 'inappropriate' pictures of children.

Everywhere you look, say photographers, digital camera enthusiasts are being turned into pariahs. However, the shutterbugs are fighting back.

MP Austin Mitchell has lodged an early day motion calling for the government to actively fight the "increase in the number of reported incidents in which the police or wardens attempt to stop street photography and order the deletion of photographs or the confiscation of cameras on various specious grounds such as claims that some public buildings are strategic or sensitive or that photographers need permission from everyone in a picture before they can take the shot".

"Photography in public places and streets is perfectly legal," he concluded.

THOUSANDS OF PEOPLE TAKE PHOTOS EVERY DAY. WHAT IF ONE OF THEM SEEMS ODD?

Terrorists use surveillance to help plan attacks, taking photos and making notes about security measures like the location of CCTV cameras. If you see someone doing that, we need to know. Let experienced officers decide what action to take.

TERRORISM. IF YOU SUSPECT IT, REPORT IT.
CALL 0800 789 321 CONFIDENTIAL ANTI-TERRORISM

▲ The rise of posters using scare tactics has put photographers on the defensive

NEWS ANALYSIS

Portrait of paranoia clouds judgement

The farrago surrounding the treatment of amateur photographers might seem of little interest to non-camera buffs, but only until you stop to consider how many photographs on your mobile phone or PC could be seen as suspicious.

Was there a public building in that snap of your kids in London?

Have you asked permission of everyone in the background and should you have asked all the parents of the youngsters sharing a fairground ride with your nipper?

The idea that you can't take pictures in a public place is preposterous. Lowry and his matchstick men? Lock 'em up. Constable and his haywain? Burn 'em. Images of street life are important snapshots of society and worth protecting in nearly all cases, except where we're talking dirty old man in a raincoat taking pictures of kids.

The restrictions being touted by security officials are made all the more frustrating by the lack of any kind of logic to back them up. The situation is indicative of authority figures who make decisions based on the vaguest understanding of technology.

The main justification for the clampdown appears to be the threat posed by terrorists running around snapping major buildings and transport hubs in search of insider knowledge. But this whole premise is flawed on more levels than a multi-storey car park.

Unless it were the biggest bluff since the Trojan horse, then the chances are that any self-respecting terrorist might possess a small camera. It's unlikely they will be taking covert pictures around Trafalgar Square with an enormous DSLR camera.

A terrorist is more likely to use a covert camera the size of a mobile phone, take photos with a long lens from a van or simply buy a postcard. Yet the more advanced your camera, the more likely you are to be stopped and questioned.

The most galling aspect of all this is that at the same time as bullying hobbyist photographers and even snap-happy day-trippers, the authorities have hundreds of thousands of cameras watching us.

CCTV cameras are seen as acceptable because they are run by established security personnel rather than amateur members of the public. And, of course, Burgess and Philby – the British intelligence service agents that were spying for the Soviet Union – never posed a threat to society when they were working within the Establishment.

Then there are the legions of webcams posted around the country, many of them focused on the very buildings that are deemed too sensitive to be photographed. Now wouldn't a webcam, which you can watch in anonymity and monitor for time-sensitive changes such as security guards clocking in, be more useful than something captured on a family day out?

The situation is made worse by the fact that there are no real guidelines for police to follow when dealing with photographers. Photographers are allowed to take pictures, unless someone decides otherwise. It's a legal minefield and a perfect breeding ground for jobsworthness that brings out the worst in anyone with epaulettes on their shoulders.

The current attitude appears to suggest that lurking behind every camera lens is a jihadist waiting to pounce. There are, of course, lots of people running around taking pictures of buildings of national importance, some of them even wearing Arabic dress. They are called tourists.



▲ Trying to stop people taking snaps in public is futile



Stewart Mitchell
Correspondent